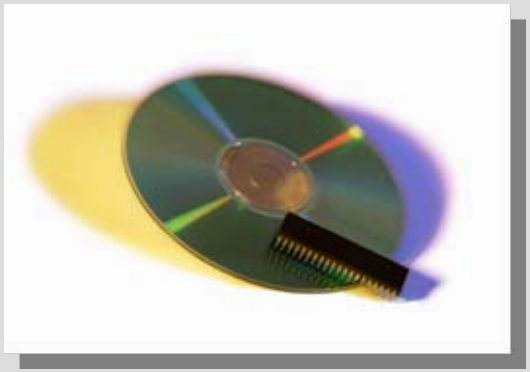
CREM Reduction Solution

Lorene Blakely
Aaron Thronas

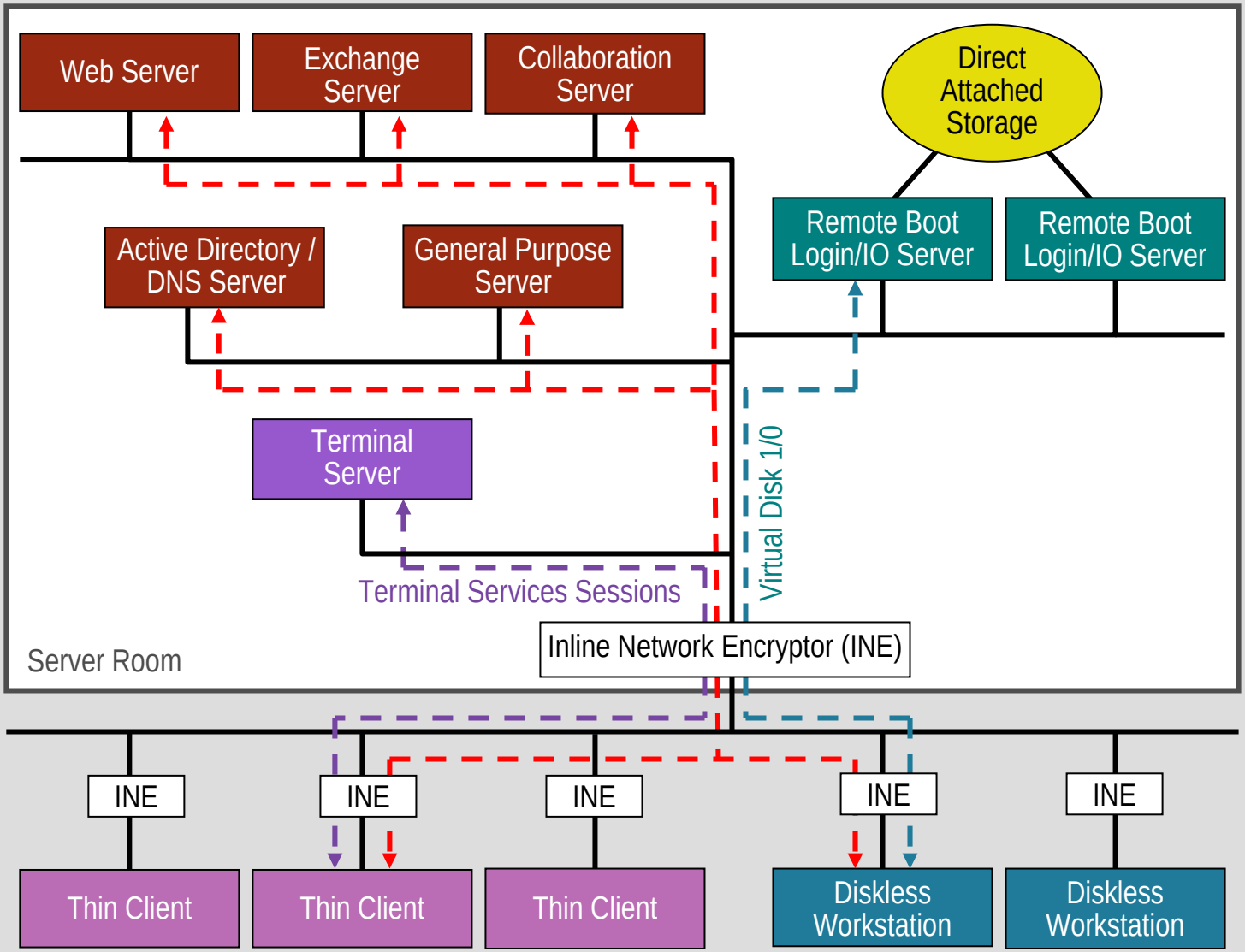
Pacific Northwest National Laboratory
PNNL-SA-49571

Background

- Driver: Classified Removable Electronic Media (CREM) Reduction Taskforce
- Current State:
  - 100 facilities (standalone, networks, clusters)
  - 150 computers
  - 1000 pieces of CREM (as reported by users)



Architecture



Network Security

- Network Infrastructure STIG
  - Securing routers and switches
  - Intrusion detection
  - Device management
  - SYSLOG
  - VLANS
- DNS STIG

Additional Security

- NSA/Microsoft security templates
  - Exchange 2003 Hardening Guide
  - Windows Server 2003 Security Guide
    - Domain controllers
    - Domain infrastructure settings
    - Creating baseline
    - Print servers
    - File servers
    - IIS servers
    - SQL servers

Systems Management

- Symantec Antivirus console
- Microsoft Systems Management Server
- Microsoft Operations Manager

Hard Security

- GSA approved security containers
- Network encryptors - Type 1 (KG-175)
  - Taclane
  - Physical layer on OSI
- Audit workstation

Server Hardware

- Dell PowerEdge 2850
  - High uptime
  - Cable management
  - Expandability
  - Internal SCSI RAID
- APC UPS
- ADIC Scalar backup tape robot
- StorCase disk array

Services

- Domain Services
  - Active Directory for centralized authentication
  - Group Policy for standardization across servers
    - NSA/Microsoft security templates
- Exchange E-Mail
  - Exchange 2003
  - Secure collaboration
  - NSA/Microsoft security templates applied specific to Exchange
  - E-mail classification marking tool

Services (continued)

- Terminal emulation
  - Citrix Presentation Server
  - More secure and featured than terminal services alone
  - Load balanced across several servers

- Host-based Intrustion Detection System/Firewall
  - Behavior-based intrusion detection system
  - Centralized logging for the IDS system

Services (continued)

- Thin/Thick client management
  - Ardence for thick client images
  - Altiris management software for thin clients
- Print services
  - Centralized management and logging for networked printers
- Log Monitoring
  - Centralized SYSLOG service for server event logs

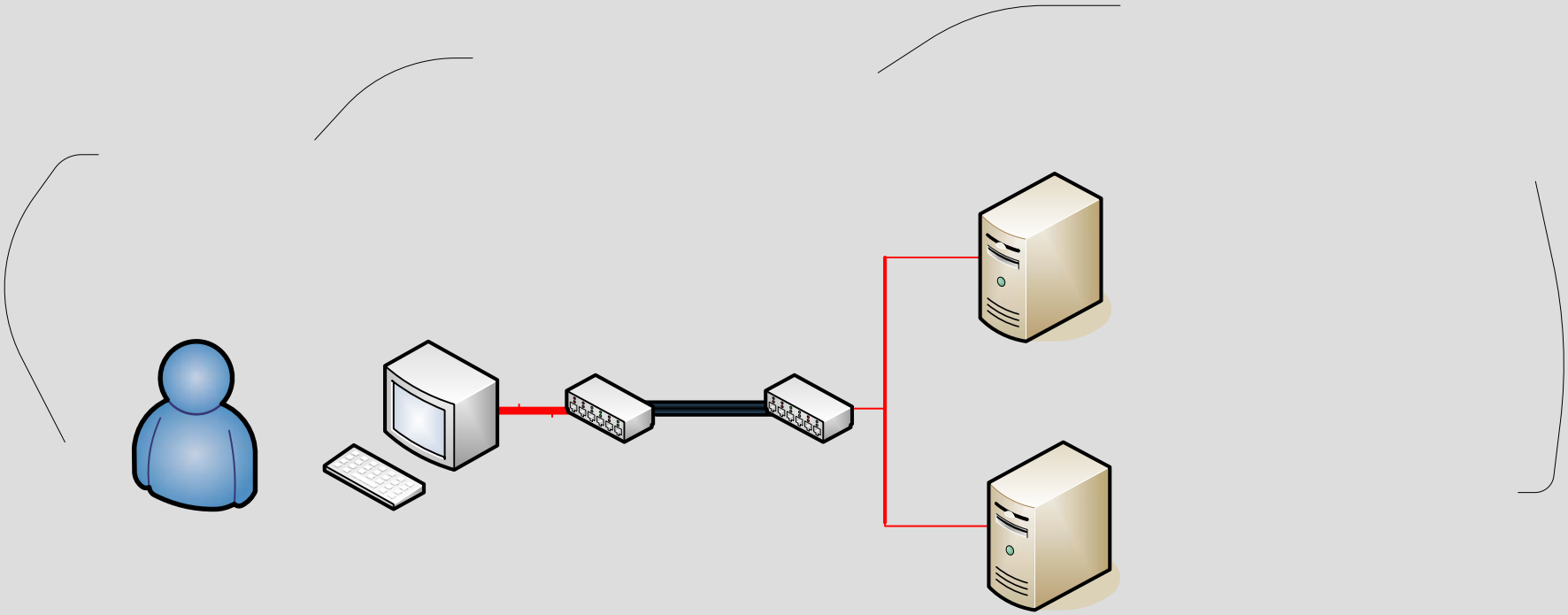
Services (continued)

- SharePoint services
- Office classification marking tools
  - E-mail
  - Office 2003 documents
- Print marking and logging
- Future services
  - Access to clusters
  - Hosting of other servers
  - Instant Messaging

Thin Client: Hardware/Software

- Hardware
  - HP Thin Client: 1.2 GHz, 512MB RAM
  - EWF (Enhanced Write Filter)
  - Read only DVD-ROM available
- Management Software
  - Altiris
- User Software Available Via Citrix
  - Microsoft Office, Internet Explorer, Windows Media Player, Quicktime, Adobe Reader, Norton Antivirus

Thin Client Startup



Thick Clients

- Dell Precision 670, dual-processor
- No hard drive
- Customizable
- Similar user experience

Thick Client Startup

1. User powers on the thick client.

2. The thick client sends MAC address to Ardence server for authentication on the network.

3. After verification of the MAC address against the allowed client list, Ardence accepts the connection.

4. Ardence identifies the thick client and sends the correct image to the machine.

5. The thick client boots to Windows XP and loads all of the customizations previously created for this thick client.

Thick Client Applications

- MatLab
- TurboCAD
- Adobe Acrobat Pro
- Adobe Photoshop
- Adobe Illustrator
- Software available via Citrix
  - Microsoft Office, Internet Explorer, Windows Media Player, Quicktime, Adobe Reader, Norton Antivirus
- Each thick client individually customizable to future needs